Toolkit para Criptoanálisis

Castro Lechtaler, Antonio[1, 2]; Cipriano, Marcelo[1,3]; García, Edith[1],
Liporace, Julio[1]; Maiorano, Ariel[1]; Malvacio, Eduardo[1]; Tapia, Néstor[1];

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Escuela Superior Técnica, Facultad del Ejército. Universidad de la Defensa Nacional - UNDEF
[2] CISTIC/FCE - Universidad de Buenos Aires.
[3] Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.

acastro@est.iue.edu.ar , marcelocipriano@est.iue.edu.ar,
{edithxgarcia; jcliporace; maiorano; edumalvacio; tapianestor87}@gmail.com

RESUMEN

El proyecto se extiende desde el estudio hasta la implementación de técnicas o métodos criptoanalíticos para ser aplicados a determinados generadores de secuencias seudoaleatorias tipo *Stream Ciphers*[1], en particular a aquellos algoritmos que involucran *LFSR´s*[2], *NLFSR´s*[3], *CCG´s* [4] y *CA´s* [5].

En particular los métodos a estudiar serán los correspondientes al *Criptoanálisis Diferencial* [1-2], Criptoanálisis *Lineal* [3], *Criptoanálisis Algebraico, Guess-and-Determine [4]* y una de las últimas y poderosas técnica de criptoanálisis publicada hace relativamente poco, denominada *Cube Attack*[6] [5].

El desarrollar un conjunto de herramientas de criptoanálisis permitirá la realización de análisis de algoritmos de cifrado, generadores de secuencias seudoaleatorias, primitivas criptológicas, protocolos de seguridad de la información, y claves secretas de distintos criptosistemas, entre otros.

[1] Stream cipher: generadores seudoaleatorios conocidos también como generadores en flujo o cadena.

[2] Linear Feedback Shift Registers: registros de desplazamiento realimentados linealmente.

[3] Non Linear Feedback Shift Registers: registros de desplazamiento realimentados no linealmente.

[4] Clock Controlled Generators: generadores controlados por reloj.

[5] Cellular Automata: autómata celular.

[6] Presentado en el congreso EuroCrypt del año 2009 por sus autores: Itai Dinur y Adi Shamir.

Palabras Clave

Criptología, Criptoanálisis. Stream Ciphers.

CONTEXTO

En el marco de la carrera de grado de Ingeniería en Informática y el posgrado en Criptografía y Seguridad Teleinformática que se dictan en la *Escuela Superior Técnica "Gral. Div. Manuel N. Savio" (EST)*, dependiente de la *Facultad del Ejército, Universidad de la Defensa Nacional (UNDEF)* se llevan adelante tareas de I+D+i por parte del *Grupo de Investigación en Criptología y Seguridad Informática (GICSI).*

GICSI depende del *Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CriptoLab)* perteneciente al *Laboratorio Informática (InforLab).* Y está conformado por docentes investigadores, profesionales técnicos y alumnos de dicha área.

1. INTRODUCCIÓN

Ya es claro que el uso masivo de las comunicaciones electrónicas ha cambiado nuestra sociedad. Desde computadoras y teléfonos inteligentes a dispositivos *smart* como televisores, electrodomésticos y otros sistemas que anexaron la comunicación a sus funciones. Es por ello que la transmisión y almacenamiento de información requiere tomar una serie de medidas de protección manteniendo su

confidencialidad, autenticidad e integridad. La falta total o parcial de medidas de seguridad se convierte en una amenaza latente.

Al momento de realizar el diseño de un criptosistema se deben tener en cuenta, obviamente, todos los ataques que éste puede sufrir. Cada aspecto en su diseño responde, entre otros criterios, a un ataque criptoanalítico, demostrando así su resistencia a él. Esta filosofía de diseño ha llevado a los modernos criptológicos a demostrar que pueden sortear diferentes amenazas, cuidadosa y eficientemente desarrolladas para atacarlos. Ya que cada algoritmo, cada primitiva, cada protocolo debe ser atacado mediante una técnica adecuada a su estructura.

Es por ello que existen diferentes y poderosas herramientas de criptoanálisis. Y todo parece indicar que se incorporarán cada vez más de ellas, en un futuro no muy lejano. De la misma manera se requerirán nuevos y probados sistemas criptográficos que resistan los ataques que van apareciendo. Y así seguirá.

Últimamente el diseño de algoritmos seguros ha tenido un gran avance. De un tiempo a esta parte, entre otros:

- el llamado en 1997 del *NIST*[7] para escoger un nuevo algoritmo como estándar de cifrado llamado *AES* [6].
- El concurso europeo e-*Stream* en 2004, organizado por el *E-CRYPT* [7] del cual superaron todas las pruebas y ataques, 7 algoritmos.
- el llamado a concurso del *NIST* para escoger un nuevo algoritmo como estándar *SHA-3*[8], finalizado en 2012. Aunque aún no se da de baja al *SHA-2* por no demostrar, hasta el momento, debilidades.
- el concurso aún en proceso *CAESAR*[9] el cual se espera que pronto se den a conocer a los finalistas y luego al ganador o un portfolio con los algoritmos elegidos[8].

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

Se ha dado en planificar este proyecto de investigación siguiendo 6 etapas:

1. Mediante el estudio de bibliografía actualizada y la asistencia a Cursos, Congresos y Workshops específicos, se profundizará en el estado del arte del Criptoanálisis y los nuevos ataques que se han desarrollado.
2. Estudio, análisis y selección de los generadores de secuencias cifrantes.
3. Relevamiento de los métodos criptoanalíticos que se analizarán.
4. Estudio de técnicas criptográficas para la determinación del o los métodos de ataque adecuados a la estructura del algoritmo estudiado.
5. Implementación de los métodos de criptoanálisis.
6. Análisis de los resultados obtenidos.

3. RESULTADOS OBTENIDOS / ESPERADOS

Se realizará el estudio, análisis y desarrollo de técnicas y/o herramientas que posibiliten la realización del diseño de aplicaciones criptográficas, su evaluación, búsqueda de

[7] Institución de Estados Unidos, llamada Instituto de Normas y Estandarización (National Institute of Standards and Technology) por sus siglas en inglés.

[8] Secure Hash Algorithm por sus siglas en inglés.

[9] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness.

vulnerabilidades y de ser posible, lograr su ataque.

Los alcances del criptoanálisis podrán ser:

- Obtención de la/s clave/s del cifrado.
- Hallar patrones estadísticos en la salida del sistema estudiado.
- Desarrollar nuevas técnicas criptoanalíticas de acuerdo a las propiedades del sistema estudiado.
- Analizar el algoritmo de generación de la/s clave/s y estudiar su vulnerabilidad.

Para ello se perseguirán los objetivos particulares:

- Estudio y análisis de técnicas criptoanalíticas.
- Diseño y desarrollo de herramientas de evaluación, ataque o quiebre de aplicaciones criptográficas.
- Pruebas y testeo de las herramientas desarrolladas sobre algoritmos específicos.

4. FORMACIÓN DE RECURSOS HUMANOS

Los docentes investigadores participantes del proyecto dictan las asignaturas *Criptografía y Seguridad Teleinformática, Matemática Discreta y Paradigmas de Programación I, II.* Desde esas cátedras se invita a los alumnos a participar en los proyectos de investigación. Es por ello que los alumnos *Dorado, Mariano, Cabrera Ezequiel, Leiras Facundo y Romero, Luciano* han demostrado su interés y se han sumado en calidad de colaboradores. En particular los dos últimos serán postulantes para la beca "Estímulo a las Vocaciones Científicas" (EVC) otorgadas por el Consejo Interuniversitario Nacional (CIN) por encuadrarse en las condiciones pedidas [9].

Se desea destacar que el incremento del Know-How que tendrá el grupo de investigadores a lo largo de la vida del proyecto será una importante y económica Formación de Recursos Humanos en beneficio de sus integrantes.

Atendiendo a la responsabilidad ética y social que compete a la actividad científica y tecnológica, el Grupo Integrante de este Proyecto de Investigación, ya sea durante su ejecución o por la aplicación de los resultados obtenidos, desea expresar su compromiso a no realizar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio ambiente, a los animales y/o a las generaciones futuras.

5. BIBLIOGRAFÍA

[1] Ding C.; *The differential cryptanalysis and design of natural stream ciphers*. In: Anderson R. (eds.) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol. 809. Springer Berlin, Heidelberg.

[2] Wu H., Preneel B. *Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy*. Naor M. (eds.) Advances in Cryptology. EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515. Springer Berlin, Heidelberg. 2007.

[3] Muller F., Peyrin T. *Linear Cryptanalysis of the TSC Family of Stream Ciphers.* Roy B. (eds.) Advances in Cryptology - ASIACRYPT 2007. Lecture Notes in Computer Science, vol. 3788. Springer, Berlin, Heidelberg. 2005.

[4] Pasalic, E.; *On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers*; IEEE Transactions on Information Theory. Vol. 55 Ed.7º, 2009.

[5] Dinur I., Shamir A. *Cube Attacks on Tweakable Black Box Polynomials.* Advances in Cryptology - EUROCRYPT 2009. Lecture Notes in Computer Sci-

ence, vol 5479. Springer, Berlin, Heidelberg. 2009.
[6] Daemen, J.; Rijmen, V.*; The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer. New York. 2002.
[7] http://www.ecrypt.eu.org/stream/ Consultada el 10-3-18.
[8] https://competitions.cr.yp.to/caesar.html. Consultada el 10-3-18.
[9]http://evc.cin.edu.ar/informacion consultada el 23/2/2018.